(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 076 975 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
14.10.2009 Bulletin 2009/42

(21) Application number: **99920165.0**

(22) Date of filing: **29.04.1999**

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(86) International application number:
PCT/US1999/009362

(87) International publication number:
WO 1999/057866 (11.11.1999 Gazette 1999/45)

(54) **USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM**

VERBRAUCHER-SPEZIFISCHES DATENWEITERLEITUNGSSYSTEM

SYSTEME DE REACHEMINEMENT AUTOMATIQUE DE DONNEES, SPECIFIQUE A L'UTILISATEUR

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **04.05.1998 US 84014 P**
21.04.1999 US 295966

(43) Date of publication of application:
21.02.2001 Bulletin 2001/08

(73) Proprietor: **Auric Web Systems**
Pasadena, CA 91107 (US)

(72) Inventors:
- **IKUDOME, Koichiro**
Arcadia, CA 91007 (US)
- **YEUNG, Moon, Tai**
Alhambra, CA 91801 (US)

(74) Representative: **Kinsler, Maureen Catherine et al**
Kilburn & Strode LLP
20 Red Lion Street
London
WC1R 4PJ (GB)

(56) References cited:
EP-A- 0 854 621
WO-A-96/05549
WO-A-98/26548
US-A- 5 696 898

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 076 975 B1

Description

FIELD OF THE INVENTION

[0001] This invention relates to the field of Internet communications, more particularly, to a database system for use in dynamically redirecting and filtering Internet traffic.

BACKGROUND OF THE INVENTION

[0002] In prior art systems as shown in FIG. 1 when an Internet user establishes a connection with an Internet Service Provider (ISP), the user first makes a physical connection between their computer 100 and a dial-up networking server 102, the user provides to the dial-up networking server their user ID and password. The dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104. A detailed description of the IP communications protocol is discussed in Internetworking with TCP/IP, 3rd ed., Douglas Comer, Prentice Hall, 1995, which is fully incorporated herein by reference. The authentication and accounting server, upon verification of the user ID and password using a database 106 would send an authorization message to the dial-up networking server 102 to allow the user to use the temporary IP address assigned to that user by the dial-up networking server and then logs the connection and assigned IP address. For the duration of that session, whenever the user would make a request to the Internet 110 via a gateway 108, the end user would be identified by the temporarily assigned IP address.

[0003] The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page - hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. Alternately, redirection can also be accomplished by coding the page such that it instructs the browser to run a program, like a Java applet or the like, which then redirects the browser. One disadvantage with current redirection technology is that control of the redirection is at the remote end, or WWW server end - and not the local, or user end. That is to say that the redirection is performed by the remote server, not the user's local gateway.

[0004] Filtering packets at the Internet Protocol (IP) layer has been possible using a firewall device or other packet filtering device for several years. Although packet filtering is most often used to filter packets coming into a private network for security purposes, once properly programed, they can filter outgoing packets sent from users to a specific destination as well. Packet filtering can distinguish, and filter based on, the type of IP service contained within an IP packet. For example, the packet filter can determine if the packet contains FTP (file transfer protocol) data, WWW data, or Telnet session data. Service identification is achieved by identifying the terminating port number contained within each IP packet header. Port numbers are standard within the industry to allow for interoperability between equipment. Packet filtering devices allow network administrators to filter packets based on the source and/or destination information, as well as on the type of service being transmitted within each IP packet. Unlike redirection technology, packet filtering technology allows control at the local end of the network connection, typically by the network administrator. However, packet filtering is very limited because it is static. Once packet filtering rule sets are programed into a firewall or other packet filter device, the rule set can only be changed by manually reprogramming the device.

[0005] Packet filter devices are often used with proxy server systems, which provide access control to the Internet and are most often used to control access to the world wide web. In a typical configuration, a firewall or other packet filtering device filters all WWW requests to the Internet from a local network, except for packets from the proxy server. That is to say that a packet filter or firewall blocks all traffic originating from within the local network which is destined for connection to a remote server on port 80 (the standard WWW port number). However, the packet filter or firewall permits such traffic to and from the proxy server. Typically, the proxy server is programed with a set of destinations that are to be blocked, and packets destined for blocked addresses are not forwarded. When the proxy server receives a packet, the destination is checked against a database for approval. If the destination is allowed, the proxy server simply forwards packets between the local user and the remote server outside the firewall. However, proxy servers are limited to either blocking or allowing specific system terminals access to remote databases.

[0006] A recent system is disclosed in U.S. patent No. 5,696,898. This patent discloses a system, similar to a proxy

server, that allows network administrators to restrict specific IP addresses inside a firewall from accessing information from certain public or otherwise uncontrolled databases (i.e., the WWW/Internet). According to the disclosure, the system has a relational database which allows network administrators to restrict specific terminals, or groups of terminals, from accessing certain locations. Similarly limited as a proxy server, this invention can only block or allow terminals' access to remote sites. This system is also static in that rules programmed into the database need to be reprogramming in order to change which locations

[0007] EP-A-0854621 discloses a system and method for providing peer-level access control, wherein the local rule base of a peer is dynamically loaded into a filter when peer is authenticated and ejected when the peer loses authentication. WO-A-9826548 discloses a device which uses an automatic configuration process to handle the task of configuring the device like a customer site for communication with the internet.

[0008] The present invention set out in the claims allows for creating and implementing dynamically changing rules to allow the redirection, blocking, or allowing, of specific data traffic for specific users, as a function of database entries and the user's activity. In certain embodiments according to the present invention, when the user connects to the local network, as in the prior art system, the user's ID and password are sent to the authentication accounting server. The user ID and password are checked against information in an authentication database. The database also contains personalized filtering and redirection information for the particular user ID. During the connection process, the dial-up network server provides the authentication accounting server with the IP address that is going to be temporarily assigned to the user. The authentication accounting server then sends both the user's temporary IP address and all of the particular user's filter and redirection information to a redirection server. The IP address temporarily assigned to the end user is then sent back to the end user for use in connecting to the network.

[0009] Once connected to the network, all data packets sent to, or received by, the user include the user's temporary IP address in the IP packet header. The redirection server uses the filter and redirection information supplied by the authentication accounting server, for that particular IP address, to either allow packets to pass through the redirection server unmolested, block the request all together, or modify the request according to the redirection information.

[0010] When the user terminates the connection with the network, the dial-up network server informs the authentication accounting server, which in turn, sends a message to the redirection server telling it to remove any remaining filtering and redirection information for the terminated user's temporary IP address. This then allows the dial-up network to reassign that IP address to another user. In such a case, the authentication accounting server retrieves the new user's filter and redirection information from the database and passes it, with the same IP address which is now being used by a different user, to the redirection server. This new user's filter may be different from the first user's filter.

FIG. 1 is a block diagram of a typical Internet Service Provider environment.

FIG. 2 is a block diagram of an embodiment of an Internet Service Provider environment with integrated redirection system.

[0011] In the following embodiments of the invention, common reference numerals are used to represent the same components. If the features of an embodiment are incorporated into a single system, these components can be shared and perform all the functions of the described embodiments.

[0012] FIG 2. shows a typical Internet Service Provider (ISP) environment with integrated user specific automatic data redirection system. In a typical use of the system, a user employs a personal computer (PC) 100, which connects to the network. The system employs: a dial-up network server 102, an authentication accounting server 204, a database 206 and a redirection server 208.

[0013] The PC 100 first connects to the dial-up network server 102. The connection is typically created using a computer modem, however a local area network (LAN) or other communications link can be employed. The dial-up network server 102 is used to establish a communications link with the user's PC 100 using a standard communications protocol. In the preferred embodiment Point to Point Protocol (PPP) is used to establish the physical link between the PC 100 and the dial-up network server 102, and to dynamically assign the PC 100 an IP address from a list of available addresses. However, other embodiments may employ different communications protocols, and the IP address may also be permanently assigned to the PC 100. Dial-up network servers 102, PPP and dynamic IP address assignment are well known in the art.

[0014] An authentication accounting server with Auto-Navi component (hereinafter, authentication accounting server) 204 is used to authenticate user ID and permit, or deny, access to the network. The authentication accounting server 204 queries the database 206 to determine if the user ID is authorized to access the network. If the authentication accounting server 204 determines the user ID is authorized, the authentication accounting server 204 signals the dial-up network server 102 to assign the PC 100 an IP address, and the Auto-Navi component of the authentication accounting server 204 sends the redirection server 208 (1) the filter and redirection information stored in database 206 for that user ID and (2) the temporarily assigned IP address for the session. One example of an authentication accounting server is discussed in U.S. Patent No. 5,845,070, which is fully incorporated here by reference. Other types of authentication

accounting servers are known in the art. However, these authentication accounting servers lack an Auto-Navi component.

[0015] The system described herein operates based on user Id's supplied to it by a computer. Thus the system does not "know" who the human being "user" is at the keyboard of the computer that supplies a user ID. However, for the purposes of this detailed description, "user" will often be used as a short hand expression for "the person supplying inputs to a computer that is supplying the system with a particular user ID."

[0016] The database 206 is a relational database which stores the system data. FIG. 3 shows one embodiment of the database structure. The database, in the preferred embodiment, includes the following fields: a user account number, the services allowed or denied each user (for example: e-mail, Telnet, FTP, WWW), and the locations each user is allowed to access.

[0017] Rule sets are employed by the system and are unique for each user ID, or a group of user ID's. The rule sets specify elements or conditions about the user's session. Rule sets may contain data about a type of service which may or may not be accessed, a location which may or may not be accessed, how long to keep the rule set active, under what conditions the rule set should be removed, when and how to modify the rule set during a session, and the like. Rule sets may also have a preconfigured maximum lifetime to ensure their removal from the system.

[0018] The redirection server 208 is logically located between the user's computer 100 and the network, and controls the user's access to the network. The redirection server 208 performs all the central tasks of the system. The redirection server 208 receives information regarding newly established sessions from the authentication accounting server 204. The Auto-Navi component of the authentication accounting server 204 queries the database for the rule set to apply to each new session, and forwards the rule set and the currently assigned IP address to the redirection server 208. The redirection server 208 receives the IP address and rule set, and is programed to implement the rule set for the IP address, as well as other attendant logical decisions such as: checking data packets and blocking or allowing the packets as a function of the rule sets, performing the physical redirection of data packets based on the rule sets, and dynamically changing the rule sets based on conditions. When the redirection server 208 receives information regarding a terminated session from the authentication accounting server 204, the redirection server 208 removes any outstanding rule sets and information associated with the session. The redirection server 208 also checks for and removes expired rule sets from time to time.

[0019] In an alternate embodiment, the redirection server 208 reports all or some selection of session information to the database 206. This information may then be used for reporting, or additional rule set generation.

System Features Overview

[0020] In the present embodiment, each specific user may be limited to, or allowed, specific IP services, such as WWW, FTP and Telnet. This allows a user, for example, WWW access, but not FTP access or Telnet access. A user's access can be dynamically changed by editing the user's database record and commanding the Auto-Navi component of the authentication accounting server 204 to transmit the user's new rule set and current IP address to the redirection server 208.

[0021] A user's access can be "locked" to only allow access to one location, or a set of locations, without affecting other users' access. Each time a locked user attempts to access another location, the redirection server 208 redirects the user to a default location. In such a case, the redirection server 208 acts either as proxy for the destination address, or in the case of WWW traffic the redirection server 208 replies to the user's request with a page containing a redirection command.

[0022] A user may also be periodically redirected to a location, based on a period of time or some other condition. For example, the user will first be redirected to a location regardless of what location the user attempts to reach, then permitted to access other locations, but every ten minutes the user is automatically redirected to the first location. The redirection server 208 accomplishes such a rule set by setting an initial temporary rule set to redirect all traffic; after the user accesses the redirected location, the redirection server then either replaces the temporary rule set with the user's standard rule set or removes the rule set altogether from the redirection server 208. After a certain or variable time period, such as ten minutes, the redirection server 208 reinstates the rule set again.

[0023] The following steps describe details of a typical user session:

- A user connects to the dial-up network server 102 through computer 100.
- The user inputs user ID and password to the dial-up network server 102 using computer 100 which forwards the information to the authentication accounting server 204
- The authentication accounting server 204 queries database 206 and performs validation check of user ID and password.
- Upon a successful user authentication, the dial-up network server 102 completes the negotiation and assigns an IP address to the user. Typically, the authentication accounting server 204 logs the connection in the database 206.
- The Auto-Navi component of the authentication accounting server 204 then sends both the user's rule set (contained

in database 206) and the user's IP address (assigned by the dial-up network server 102) in real time to the redirection server 208 so that it can filter the user's IP packets.

• The redirection server 208 programs the rule set and IP address so as to control (filter, block, redirect, and the like) the user's data as a function of the rule set.

[0024] The following is an example of a typical user's rule set, attendant logic and operation:

[0025] If the rule set for a particular user (i.e., user UserID-2) was such as to only allow that user to access the web site www.us.com, and permit Telnet services, and redirect all web access from any server at xyz.com to www.us.com, then the logic would be as follows:

[0026] The database 206 would contain the following record for user UserID-2:

```
ID                  UserID-2
Password:           secret

################
### Rule Sets ###
################

#service    rule                    expire
http        www.us.com              0
http        *.xyz.com=>www.us.com   0
```

• the user initiates a session, and sends the correct user ID and password (UserID-2 and secret) to the dial-up network server 102. As both the user ID and password are correct, the authentication accounting server 204 authorizes the dial-up network server 102 to establish a session. The dial-up network server 102 assigns UserID-2 an IP address (for example, 10.0.0.1) to the user and passes the IP address to the authentication accounting server 204.

• The Auto-Navi component of the authentication accounting server 204 sends both the user's rule set and the user's IP address (10.0.0.1) to the redirection server 208.

• The redirection server 208 programs the rule set and IP address so as to filter and redirect the user's packets according to the rule set. The logic employed by the redirection server 208 to implement the rule set is as follows:

```
IF source IP-address = 10.0.0.1 AND
    (   ((request type = HTTP) AND (destination address = www.us.com) ) OR
        (request type = Telnet)
    )   THEN ok.

IF source IP-address = 10.0.0.1 AND
    (   (request type = HTTP) AND (destination address = *.xyz.com)
    )   THEN (redirect = www.us.com)
```

[0027] The redirection server 208 monitors all the IP packets, checking each against the rule set. In this situation, if IP address 10.0.0.1 (the address assigned to user ID UserID-2) attempts to send a packet containing HTTP data (i.e., attempts to connect to port 80 on any machine within the xyz.com domain) the traffic is redirected by the redirection server 208 to www.us.com. Similarly, if the user attempts to connect to any service other then HTTP at www.us.com or Telnet anywhere, the packet will simply be blocked by the redirection server 208.

[0028] When the user logs out or disconnects from the system, the redirection server will remove all remaining rule sets.

[0029] The following is another example of a typical user's rule set, attendant logic and operation:

[0030] If the rule set for a particular user (i.e., user UserID-3) was to force the user to visit the web site www.widget-sell.com, first, then to have unfettered access to other web sites, then the logic would be as follows:

The database 206 would contain the following record for user UserID-3:

```
ID                  UserID-3
Password:           top-secret

################
### Rule Sets ###
################

#service    rule                      expire
http        *=>www.widgetsell.com     1x
```

- the user initiates a session, and sends the correct user ID and password (UserID-3 and top-secret) to the dial-up network server 102. As both the user ID and password are correct, the authentication accounting server 204 authorizes the dial-up network server 102 to establish a session. The dial-up network server 102 assigns user ID 3 an IP address (for example, 10.0.0.1) to the user and passes the IP address to the authentication accounting server 204.

- The Auto-Navi component of the authentication accounting server 204 sends both the user's rule set and the user's IP address (10.0.0.1) to the redirection server 208.

- The redirection server 208 programs the rule set and IP address so as to filter and redirect the user's packets according to the rule set. The logic employed by the redirection server 208 to implement the rule set is as follows:

```
IF source IP-address = 10.0.0.1 AND
      (request type = HTTP) THEN (redirect = www.widgetsell.com)

THEN SET NEW RULE
 IF source IP-address = 10.0.0.1  AND
      (request type = HTTP)  THEN ok.
```

[0031] The redirection server 208 monitors all the IP packets, checking each against the rule set. In this situation, if IP address 10.0.0.1 (the address assigned to user ID UserID-3) attempts to send a packet containing HTTP data (i.e., attempts to connect to port 80 on any machine) the traffic is redirected by the redirection server 208 to www.widgetsell.com. Once this is done, the redirection server 208 will remove the rule set and the user if free to use the web unmolested.

[0032] When the user logs out or disconnects from the system, the redirection server will remove all remaining rule sets.

[0033] In an alternate embodiment a user may be periodically redirected to a location, based on the number of other factors, such as the number of locations accessed, the time spent at a location, the types of locations accessed, and other such factors.

[0034] A user's account can also be disabled after the user has exceeded a length of time. The authentication accounting server 204 keeps track of user's time online. Prepaid use subscriptions can thus be easily managed by the authentication accounting Server 204.

[0035] In yet another embodiment, signals from the Internet 110 side of redirection server 208 can be used to modify rule sets being used by the redirection server. Preferably, encryption and/or authentication are used to verify that the server or other computer on the Internet 110 side of redirection server 208 is authorized to modify the rule set or rule sets that are being attempted to be modified. An example of this embodiment is where it is desired that a user be redirected to a particular web site until the fill out a questionnaire or satisfy some other requirement on such a web site.

In this example, the redirection server redirects a user to a particular web site that includes a questionnaire. After this web site receives acceptable data in all required fields, the web site then sends an authorization to the redirection server that deletes the redirection to the questionnaire web site from the rule set for the user who successfully completed the questionnaire. Of course, the type of modification an outside server can make to a rule set on the redirection server is not limited to deleting a redirection rule, but can include any other type of modification to the rule set that is supported by the redirection server as discussed above.

[0036] It will be clear to one skilled in the art that the invention may be implemented to control (block, allow and redirect) any type of service, such as Telnet, FTP, WWW and the like. The invention is easily programmed to accommodate new services or networks and is not limited to those services and networks (e.g., the Internet) now know in the art.

[0037] It will also be clear that the invention may be implemented on a non-IP based networks which implement other addressing schemes, such as IPX, MAC addresses and the like. While the operational environment detailed in the preferred embodiment is that of an ISP connecting users to the Internet, it will be clear to one skilled in the art that the invention may be implemented in any application where control over users' access to a network or network resources is needed, such as a local area network, wide area network and the like. Accordingly, neither the environment nor the communications protocols are limited to those discussed.

Claims

1. A redirection server (208) connectable between a user computer (100) and a public network (110), the redirection server programmed with a user's rule set correlated to a temporarily assigned network address for the user computer, wherein the rule set contains at least one of a plurality of functions used to control the data passing between the user computer and the public network, the redirection server charcterised by being configured to allow modification of at least a portion of the rule set in the redirection server while the rule set remains correlated to the temporarily assigned network address.

2. The redirection server of claim 1, wherein the redirection server (208) is configured to allow modification of at least a portion of the rule set as a function of time.

3. The redirection server of claim 1, wherein the redirection server (208) is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

4. The redirection server of claim 1, wherein the redirection server (208) is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user access.

5. The redirection server of claim 1, wherein the redirection server (208) is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user access.

6. The redirection server of claim 1, wherein the redirection server (208) is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

7. The redirection server of claim 1, wherein the redirection server (208) is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

8. The redirection server of claim 1, wherein the redirection server (208) is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user access.

9. The redirection server of claim 1, wherein the redirection server (208) is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user access.

10. The redirection server of claim 1, wherein the redirection server (208) further blocks the data to and from the user computer (100) as a function of the rule set.

11. The redirection server of claim 1, wherein the redirection server (208) further allows the data to and from the user computer (100) as a function of the rule set.

12. The redirection server of claim 1, wherein the redirection server (208) further redirects the data to and from the user computer (100) as a function of the rule set.

13. The redirection server of claim 12, wherein the redirection server (208) redirects data from the user computer (100) by replacing a destination address in data sent from the user computer with a different destination address before the data is passed to the public network (110).

14. The redirection server of claim 1, wherein the redirection server (208) further redirects the data from the user computer (100) to multiple destinations as a function of the rule set.

15. A method for use in a redirection server (208) connected between a user computer (100) and a public network (110), the redirection server containing a user's rule set correlated to a temporarily assigned network address for the user computer wherein the user's rule set contains at least one of a plurality of functions used to control the data passing the user computer and the public network; the method **characterised by**:

    modifying at least a portion of the user's rule set in the redirection server while the user's rule set remains correlated to the temporarily assigned network address.

16. The method of claim 15, further including the step of blocking the data to and from the user computer (100) as a function of the user's rule set.

17. The method of claim 15, further including the step of allowing the data to and from the user computer (100) as a function of the user's rule set.

18. The method of claim 15, further including the step of redirecting the data to and from the user computer (100) as a function of the user's rule set.

19. The method of claim 18, wherein the step of redirecting the data from the user computer (100) comprises replacing a destination address in data sent from the user computer with a different destination address before the data is passed to the public network (110).

20. The method of claim 15, further including the step of redirecting the data from the user computer (100) to multiple destinations a function of the user's rule set.

21. The method of claim 15, further including the step of modifying at least a portion of the rule set as a function of time.

22. The method of claim 15 or claim 21, further including the step of modifying at least a portion of the rule set as a function of the data transmitted to or from the user.

23. The method of any of claims 15, 21 and 22, further including the step of modifying at least a portion of the rule set as a function of the location or locations the user access.

24. The method of claim 15, further including the step of removing or reinstating at least a portion of the user's rule set as a function of time.

25. The method of claim 15 or claim 24, further including the step of removing or reinstating at least a portion of the user's rule set as a function of the data transmitted to or from the user.

26. The method of any of claims 15, 24 and 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of the location or locations the user access.

Patentansprüche

1. Umleitungsserver (208), der zwischen einem Benutzercomputer (100) und einem öffentlichen Netz (110) anschließbar ist, wobei der Umleitungsserver mit einem Benutzer-Regelsatz programmiert ist, der mit einer temporär zugeordneten Netzadresse für den Benutzercomputer korreliert ist, wobei der Regelsatz zumindest eine einer Mehrzahl von Funktionen enthält, die zum Kontrollieren der zwischen dem Benutzercomputer und dem öffentlichen Netz

übermittelten Daten verwendet wird, wobei der Umleitungsserver **dadurch gekennzeichnet ist, dass** er eingerichtet ist, um eine Modifikation zumindest eines Teils des Regelsatzes im Umleitungsserver zu ermöglichen, während der Regelsatz mit der temporär zugeordneten Netzadresse korreliert bleibt.

2. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) eingerichtet ist, um eine Modifikation zumindest eines Teils des Regelsatzes als Funktion der Zeit zu ermöglichen.

3. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) eingerichtet ist, um eine Modifikation zumindest eines Teils des Regelsatzes als Funktion der vom Benutzer oder an diesen übertragenen zu Daten ermöglichen.

4. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) eingerichtet ist, um eine Modifikation zumindest eines Teils des Regelsatzes als Funktion des Orts oder der Orte, auf den bzw. die der Benutzer zugreift, zu ermöglichen.

5. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) eingerichtet ist, um eine Modifikation zumindest eines Teils des Regelsatzes als Funktion einer Kombination aus Zeit, vom Benutzer oder an diesen übertragenen Daten oder dem Ort oder den Orten, auf den bzw. die der Benutzer zugreift, zu ermöglichen.

6. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) eingerichtet ist, um die Entfernung oder Wiederherstellung zumindest eines Teils des Regelsatzes als Funktion der Zeit zu ermöglichen.

7. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) eingerichtet ist, um die Entfernung oder Wiederherstellung zumindest eines Teils des Regelsatzes als Funktion der vom Benutzer oder an diesen übertragenen Daten zu ermöglichen.

8. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) eingerichtet ist, um die Entfernung oder Wiederherstellung zumindest eines Teils des Regelsatzes als Funktion des Orts oder der Orte, auf den bzw. die der Benutzer zugreift, zu ermöglichen.

9. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) eingerichtet ist, um die Entfernung oder Wiederherstellung zumindest eines Teils des Regelsatzes als Funktion einer Kombination aus Zeit, vom Benutzer oder an diesen übertragenen Daten oder dem Ort oder den Orten, auf den bzw. die der Benutzer zugreift, zu ermöglichen.

10. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) weiters die Daten zum und vom Benutzercomputer (100) als Funktion des Regelsatzes blockiert.

11. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) weiters die Daten zum und vom Benutzercomputer (100) als Funktion der Regelsatzes zulässt.

12. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) weiters die Daten zum und vom Benutzercomputer (100) als Funktion des Regelsatzes umleitet.

13. Umleitungsserver nach Anspruch 12, wobei der Umleitungsserver (208) Daten vom Benutzercomputer (100) durch Ersetzen der Zieladresse in den vom Benutzercomputer gesendeten Daten durch eine andere Zieladresse umleitet, bevor die Daten in das öffentliche Netzwerk (110) gelangen.

14. Umleitungsserver nach Anspruch 1, wobei der Umleitungsserver (208) weiters die Daten vom Benutzercomputer (100) als Funktion des Regelsatzes auf mehrere Ziele umleitet.

15. Verfahren zur Verwendung in einem Umleitungsserver (208), der zwischen einem Benutzercomputer (100) und einem öffentlichen Netz (110) anschließbar ist, wobei der Umleitungsserver einen Benutzer-Regelsatz enthält, der mit einer temporär zugeordneten Netzadresse für den Benutzercomputer korreliert ist, wobei der Benutzer-Regelsatz zumindest eine einer Mehrzahl von Funktionen enthält, die zum Kontrollieren der zwischen dem Benutzercomputer und dem öffentlichen Netz übermittelten Daten verwendet wird; wobei das Verfahren **gekennzeichnet ist durch**:

Modifizieren zumindest eines Teils des Benutzer-Regelsatzes im Umleitungsserver, während der Benutzer-Regelsatz mit der temporär zugeordneten Netzadresse korreliert bleibt.

16. Verfahren nach Anspruch 15, weiters mit dem Schritt des Blockierens der Daten zum und vom Benutzercomputer (100) als Funktion des Benutzer-Regelsatzes.

17. Verfahren nach Anspruch 15, weiters mit dem Schritt des Zulassens von Daten zum und vom Benutzercomputer (100) als Funktion des Benutzer-Regelsatzes.

18. Verfahren nach Anspruch 15, weiters mit dem Schritt des Umleitens der Daten zum und vom Benutzercomputer (100) als Funktion des Benutzer-Regelsatzes.

19. Verfahren nach Anspruch 18, wobei der Schritt des Umleitens der Daten vom Benutzercomputer (100) das Ersetzen einer Zieladresse in den vom Benutzercomputer gesendeten Daten durch eine andere Zieladresse, bevor die Daten in das öffentliche Netz (110) gelangen, umfasst.

20. Verfahren nach Anspruch 15, weiters mit dem Schritt des Umleitens der Daten vom Benutzercomputer (100) zu mehreren Zielen als Funktion des Benutzer-Regelsatzes.

21. Verfahren nach Anspruch 15, weiters mit dem Schritt des Modifizierens zumindest eines Teils des Regelsatzes als Funktion der Zeit.

22. Verfahren nach Anspruch 15 oder 21, weiters mit dem Schritt des Modifizierens zumindest eines Teils des Regelsatzes als Funktion der zum oder vom Benutzer übertragenen Daten.

23. Verfahren nach einem der Ansprüche 15, 21 und 22, weiters mit dem Schritt des Modifizierens zumindest eines Teils des Regelsatzes als Funktion des Orts oder der Orte, auf den bzw. die der Benutzer zugreift.

24. Verfahren nach Anspruch 15, weiters mit dem Schritt des Entfernens oder Wiederherstellens zumindest eines Teils des Benutzer-Regelsatzes als Funktion der Zeit.

25. Verfahren nach Anspruch 15 oder 24, weiters mit dem Schritt des Entfernens oder Wiederherstellens zumindest eines Teils des Benutzer-Regelsatzes als Funktion der zum oder vom Benutzer übertragenen Daten.

26. Verfahren nach einem der Ansprüche 15, 24 und 25, weiters mit dem Schritt des Entfernens oder Wiederherstellens zumindest eines Teils des Benutzer-Regelsatzes als Funktion des Orts oder der Orte, auf den bzw. die der Benutzer zugreift.

Revendications

1. Serveur de réacheminement (208) pouvant être connecté entre un ordinateur d'utilisateur (100) et un réseau public (110), le serveur de réacheminement étant programmé avec un ensemble de règles d'un utilisateur corrélé à une adresse de réseau assignée temporairement pour l'ordinateur d'utilisateur, dans lequel l'ensemble de règles contient au moins l'une d'une pluralité de fonctions utilisées pour commander les données passant entre l'ordinateur d'utilisateur et le réseau public, le serveur de réacheminement étant **caractérisé en ce qu'**il est configuré pour permettre la modification d'au moins une partie de l'ensemble de règles dans le serveur de réacheminement alors que l'ensemble de règles reste corrélé à l'adresse de réseau assignée temporairement.

2. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) est configuré pour permettre la modification d'au moins une partie de l'ensemble de règles en fonction du temps.

3. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) est configuré pour permettre la modification d'au moins une partie de l'ensemble de règles en fonction des données transmises à destination ou en provenance de l'utilisateur.

4. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) est configuré pour permettre la modification d'au moins une partie de l'ensemble de règles en fonction de l'emplacement ou des emplacements de l'accès d'utilisateur.

5. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) est configuré

pour permettre la modification d'au moins une partie de l'ensemble de règles en fonction d'une certaine combinaison de temps, de données transmises à destination ou en provenance de l'utilisateur, ou de l'emplacement ou des emplacements de l'accès d'utilisateur

6. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) est configuré pour permettre la suppression ou le rétablissement d'au moins une partie de l'ensemble de règles en fonction du temps.

7. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) est configuré pour permettre la suppression ou le rétablissement d'au moins une partie de l'ensemble de règles en fonction des données transmises à destination ou en provenance de l'utilisateur.

8. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) est configuré pour permettre la suppression ou le rétablissement d'au moins une partie de l'ensemble de règles en fonction de l'emplacement ou des emplacements de l'accès d'utilisateur.

9. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) est configuré pour permettre la suppression ou le rétablissement d'au moins une partie de l'ensemble de règles en fonction d'une certaine combinaison de temps, de données transmises à destination ou en provenance de l'utilisateur, ou de l'emplacement ou des emplacements de l'accès d'utilisateur.

10. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) bloque en outre les données à destination et en provenance de l'ordinateur d'utilisateur (100) en fonction de l'ensemble de règles.

11. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) autorise en outre les données à destination et en provenance de l'ordinateur d'utilisateur (100) en fonction de l'ensemble de règles.

12. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) réachemine en outre les données à destination et en provenance de l'ordinateur d'utilisateur (100) en fonction de l'ensemble de règles.

13. Serveur de réacheminement selon la revendication 12, dans lequel le serveur de réacheminement (208) réachemine des données de l'ordinateur d'utilisateur (100) en remplaçant une adresse de destination dans les données envoyées de l'ordinateur d'utilisateur par une adresse de destination différente avant que les données ne soient transmises au réseau public (110).

14. Serveur de réacheminement selon la revendication 1, dans lequel le serveur de réacheminement (208) réachemine les données de l'ordinateur d'utilisateur (100) à de multiples destinations en fonction de l'ensemble de règles.

15. Procédé destiné à une utilisation dans un serveur de réacheminement (208) connecté entre un ordinateur d'utilisateur (100) et un réseau public (110), le serveur de réacheminement contenant un ensemble de règles d'un utilisateur corrélé à une adresse de réseau assignée temporairement pour l'ordinateur d'utilisateur, dans lequel l'ensemble de règles de l'utilisateur contient au moins l'une d'une pluralité de fonctions utilisées pour commander les données passant entre l'ordinateur d'utilisateur et le réseau public, le procédé étant **caractérisé par** l'étape consistant à :

modifier au moins une partie de l'ensemble de règles de l'utilisateur dans le serveur de réacheminement alors que l'ensemble de règles de l'utilisateur reste corrélé à l'adresse de réseau assignée temporairement.

16. Procédé selon la revendication 15, comprenant en outre l'étape consistant à bloquer les données à destination et en provenance de l'ordinateur d'utilisateur (100) en fonction de l'ensemble de règles de l'utilisateur.

17. Procédé selon la revendication 15, comprenant en outre l'étape consistant à autoriser les données à destination et en provenance de l'ordinateur d'utilisateur (100) en fonction de l'ensemble de règles de l'utilisateur.

18. Procédé selon la revendication 15, comprenant en outre l'étape consistant à réacheminer les données à destination et en provenance de l'ordinateur d'utilisateur (100) en fonction de l'ensemble de règles de l'utilisateur.

19. Procédé selon la revendication 18, dans lequel l'étape de réacheminement des données en provenance de l'ordinateur d'utilisateur (100) comprend le remplacement d'une adresse de destination dans les données envoyées de l'ordinateur d'utilisateur par une adresse de destination différente avant que les données ne soient transmises au réseau public (110).

20. Procédé selon la revendication 15, comprenant en outre l'étape consistant à réacheminer les données en provenance de l'ordinateur d'utilisateur (100) vers de multiples destinations en fonction de l'ensemble de règles de l'utilisateur.

21. Procédé selon la revendication 15, comprenant en outre l'étape consistant à modifier au moins une partie de l'ensemble de règles en fonction du temps.

22. Procédé selon la revendication 15 ou la revendication 21, comprenant en outre l'étape consistant à modifier au moins une partie de l'ensemble de règles en fonction des données transmises à destination ou en provenance de l'utilisateur.

23. Procédé selon l'une quelconque des revendications 15, 21 et 22, comprenant en outre l'étape consistant à modifier au moins une partie de l'ensemble de règles en fonction de l'emplacement ou des emplacements de l'accès d'utilisateur.

24. Procédé selon la revendication 15, comprenant en outre l'étape consistant à supprimer ou rétablir au moins une partie de l'ensemble de règles de l'utilisateur en fonction du temps.

25. Procédé selon la revendication 15 ou la revendication 24, comprenant en outre l'étape consistant à supprimer ou rétablir au moins une partie de l'ensemble de règles de l'utilisateur en fonction des données transmises à destination ou en provenance de l'utilisateur.

26. Procédé selon l'une quelconque des revendications 15, 24 et 25, comprenant en outre l'étape consistant à supprimer ou rétablir au moins une partie de l'ensemble de règles de l'utilisateur en fonction de l'emplacement ou des emplacements de l'accès d'utilisateur.

FIG. 1

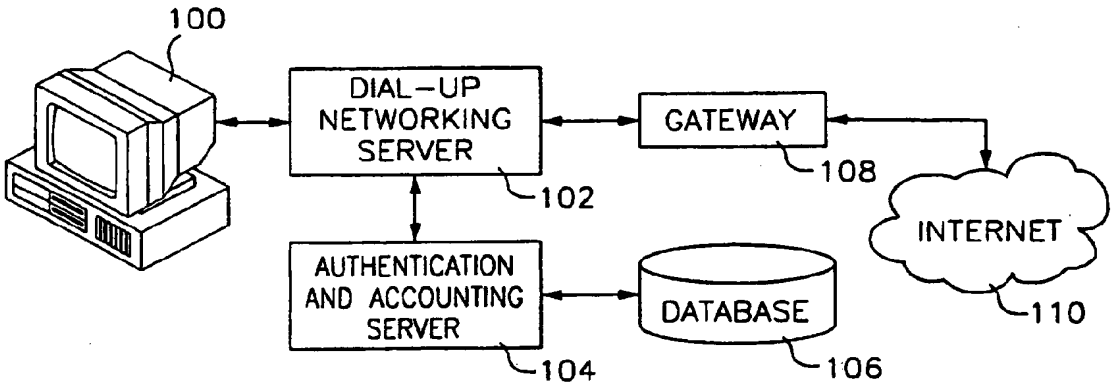
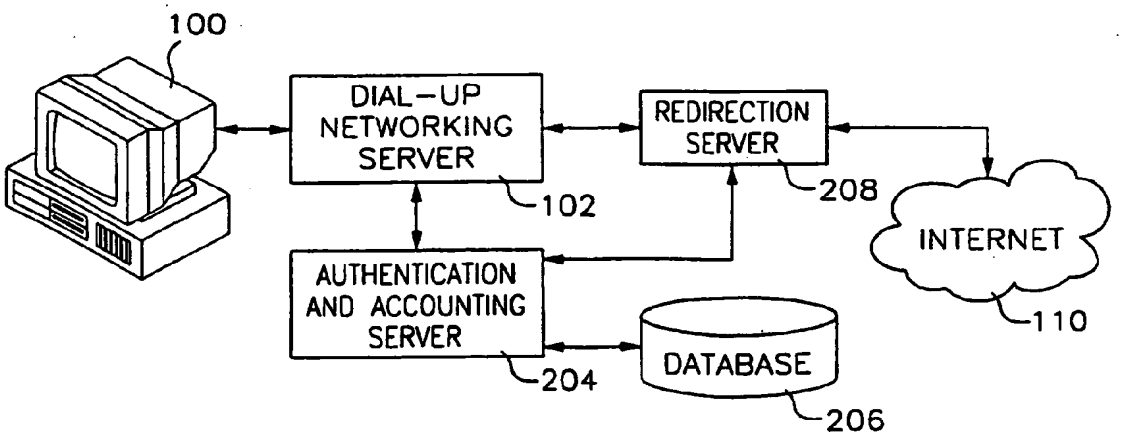

100
DIAL–UP NETWORKING SERVER
102
GATEWAY
108
INTERNET
110
AUTHENTICATION AND ACCOUNTING SERVER
104
DATABASE
106

FIG. 2


100
DIAL–UP NETWORKING SERVER
102
REDIRECTION SERVER
208
INTERNET
110
AUTHENTICATION AND ACCOUNTING SERVER
204
DATABASE
206

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 5696898 A **[0006]**
- EP 0854621 A **[0007]**
- WO 9826548 A **[0007]**
- US 5845070 A **[0014]**

Non-patent literature cited in the description

- **Douglas Comer.** Internetworking with TCP/IP. Prentice Hall, 1995 **[0002]**